SA4500 FIPS AND SA6500 FIPS SSL VPN APPLIANCES

Product Overview

Government agencies and their IT staff are chartered with reconciling seemingly opposing goals: provide reliable and timely information access to government employees and citizens while protecting sensitive resources. Federal agencies are further directed to procure only those IT technologies that meet the rigors of government communication standards and have been certified to that effect. While these strictures are actually required for some government agencies, they also provide useful guidelines to private sector businesses that require stringent security. Juniper Networks uniquely delivers on these needs with proven solutions that provide the most flexible secure access available among U. S. government-certified solutions.

Product Description

Juniper Networks® is the market leader in SSL-based remote access that is easy to deploy and easy to maintain. All Juniper Networks SA Series SSL VPN Appliances have met or exceeded the stringent security standards of independent Internet security auditing agencies. Juniper extends this leadership with a FIPS-certified hardware security module that is Federal Information Processing Standards (FIPS)-compliant. Like all SA Series appliances, the Juniper Networks SA4500 FIPS and SA6500 FIPS SSL VPN Appliances provide a hardened security gateway that uses the standards-based SSL protocol to provide remote access via a Web browser. There are no hardware or software clients to deploy, configure, or install; no changes required for internal servers; no Network Address Translation (NAT) or firewall traversal issues to manage; and virtually no ongoing maintenance. SSL itself is the most widely deployed security protocol in the world, securing billions of dollars in online banking and e-commerce transactions. The combination of these features adds up to a solution with unbeatable security, radically lower total cost of ownership (TCO) when compared to traditional VPNs or custom extranets, and a highly scalable implementation.

Please note that the FIPS models will not support Junos Pulse.

Architecture and Key Components

FIPS Security

- Stringent security with FIPS-certified Hardware Security Module (HSM) and FIPS-certified Layer 3 connectivity using Network Connect client on Windows platforms

Rich Access Privilege Management Capabilities

- Dynamic, controlled access at the URL, file, application, and server level based on a variety of session-specific variables including identity, device, security control, and network trust level

Provision by Purpose

- Three different access methods that allow administrators to balance security and access on a per-user, per-session basis

End-to-End Layered Security

- Numerous security options from the end user device to the application data and servers, including coordinated threat control with Juniper Networks IDP Series Intrusion Detection and Prevention Appliances
- Native functionality, client- and server-side APIs, and advanced malware protection capabilities for effective enforcement and unified administration of best-of-breed endpoint security

Performance Scalability with SA6500 FIPS

- A variety of performance enhancing features, including a hardware-based SSL acceleration module, and clustering to provide optimal scalability
- Up to 3,500 concurrent users supported on a single unit; up to 10,000 concurrent users supported on a four-unit cluster
- Dual, hot swappable hard drives and dual, hot swappable fans
- Hot swappable power supplies (second power supply optional, DC power supplies available)
- 4 gigabyte SDRAM
- 4-port copper 10/100/1000 interface card and 1-port copper 10/100/1000 management interface

High Availability (HA)

- Cluster pair deployment option for HA across the LAN and the WAN

Streamlined Manageability

- Central management option for unified administration
- User self service features that enhance productivity while lowering administrative overhead

Lower Total Cost of Ownership (TCO)

- Secure remote access with no client software deployments or changes to servers, and virtually no ongoing maintenance
- Secure extranet access with no demilitarized zone (DMZ) buildout, server hardening, resource duplication, or incremental deployments to add applications or users

Features and Benefits

FIPS Security

The SA4500 FIPS and SA6500 FIPS appliances incorporate a FIPS-certified HSM. The HSM handles cryptographic processing as well as key and certificate management in a hardened, tamper-proof hardware module. The HSM provides the additional benefit of offloading cryptographic processing from the host CPU, thus optimizing overall system performance while adding a physical layer of security. The SA4500 FIPS and SA6500 FIPS appliances also have a tamper evident label that deters physical security breaches and provides visual indication of appliance integrity.

Table 1: SA4500 FIPS and SA6500 FIPS Security

FEATURE	FEATURE DESCRIPTION	BENEFIT
FIPS140-2 Level 3 Certified for the Hardware Security Module & Network Connect Client	• Complies with the latest U.S. Government best practices. • FIPS140-2 is recognized by CESG as meeting security criteria for use in data traffic categorized as "Private." (CESG is the UK Government's National Technical Authority for Information Assurance, responsible for enabling secure and trusted knowledge.)	Advanced protection to provide the most stringent security.

Provision by Purpose

The SA4500 FIPS and SA6500 FIPS appliances include three different access methods. These different methods are selected as part of the user's role, allowing the administrator to enable the appropriate access on a per-session basis, taking into account user, device, and network attributes in combination with enterprise security policies.

Table 2: SA4500 FIPS and SA6500 FIPS Provision by Purpose

FEATURE	FEATURE DESCRIPTION	BENEFIT
Clientless core Web access	• Access to web-based applications, including complex JavaScript, XML, or Flash-based apps and Java applets that require a socket connection, as well as standards-based email like Outlook Web Access (OWA), Windows and UNIX file share, telnet/SSH hosted applications, terminal emulation, Sharepoint, and others. • Core Web access also enables the delivery of Java applets directly from the SA4500 FIPS or SA6500 FIPS appliance.	Provides the most easily accessible form of application and resource access, and enables extremely granular security control options; completely clientless approach using only a Web browser.
Secure Application Manager (SAM)	• A lightweight Java or Windows-based download enables access to client/server applications. Also provides native access to terminal server applications without the need for a preinstalled client.	Enables access to client/server applications using just a Web browser; no client software is necessary.
Network Connect	• Provides complete network-layer connectivity via an automatically provisioned cross-platform download. • Users need only a Web browser.	On the FIPS models, Network Connect provides SSL VPN based transport mode for layer 3 connectivity to the corporate network.

Access Privilege Management Capabilities

The SA4500 FIPS and SA6500 FIPS appliances provide dynamic access privilege management capabilities without infrastructure changes, custom development, or software deployment/maintenance. This facilitates the easy deployment and maintenance of secure remote access, as well as secure extranets and intranets. When a user logs into an SA4500 FIPS or SA6500 FIPS appliance, they pass through a pre-authentication assessment, and are then dynamically mapped to the session role that combines established network, device, identity, and session policy settings. Granular resource authorization policies further ensure exact compliance to security strictures.

Table 3: SA4500 FIPS and SA6500 FIPS Access Privilege Management Capabilities

FEATURE	FEATURE DESCRIPTION	BENEFIT
User-Record Synchronization	Supports synchronization of user records such as user bookmarks across different non-clustered SA Series appliances.	Ensures ease of experience for users who often travel from one region to another and therefore need to connect to different SA Series appliances.
VDI (Virtual Desktop Infrastructure) Support	Allows interoperability with VMware View Manager and Citrix XenDesktop to enable administrators to deploy virtual desktops with the SA Series appliances.	Provides seamless access to remote users to their virtual desktops hosted on VMware or Citrix servers. Provides dynamic delivery of the Citrix ICA client or the VMware View client, including dynamic client fallback options to allow users to easily connect to their virtual desktops.
ActiveSync Feature	Provides secure access connectivity from mobile devices (such as Symbian, Windows Mobile, or iPhone) to the Exchange server with no client software installation. Enables up to 5000 simultaneous sessions on the SA6500.	Simplifies the end-user experience when they are using a mobile device to get network access.
Hybrid role/resource-based policy model	Administrators can tailor access.	Ensures that security policies reflect changing business requirements.
Pre-authentication assessment	Network and device attributes, including presence of Host Checker/Cache Cleaner, results of endpoint security scans, source IP, browser type, and digital certificates can be examined even before login is allowed.	Results can be used in dynamic policy enforcement decisions.
Dynamic authentication policy	Enables administrators to establish a dynamic authentication policy for each unique session.	Leverages the enterprise's existing investment in directories, public key infrastructure (PKI), and strong authentication.
Dynamic role mapping	Combines network, device, and session attributes to determine which of three different types of access is allowed.	Enables the administrator to provision by purpose for each unique session.
Resource authorization	Provides extremely granular access control to the URL, server or file level.	Allows administrators to tailor security policies to specific groups, providing access only to essential data.
Granular auditing and logging	Can be configured at the per user, per resource, and per event level for security purposes as well as capacity planning.	Provides fine-grained auditing and logging capabilities in a clear, easy to understand format.
Custom expressions	Enables the dynamic combination of attributes on a "per session" basis, at the role definition/mapping rules and the resource authorization policy level.	Enables finer granularity and customization of policy roles.

End-to-End Layered Security

The SA4500 FIPS and SA6500 FIPS appliances provide complete, end-to-end layered security, including endpoint client, device, data, and server layered security controls. These include:

Table 4: SA4500 FIPS and SA6500 FIPS End-to-End Layered Security

FEATURE	FEATURE DESCRIPTION	BENEFIT
UAC-SA Federation	Seamlessly provision SA Series user sessions into Juniper Networks Unified Access Control (UAC) upon login—or the alternative (provisioning of UAC sessions into the SA Series). Users need to authenticate only one time to get access in these types of environments.	Provides users—whether remote or local—seamless access with a single login to corporate resources which are protected by access control policies from UAC or the SA Series. Simplifies end-user experience.
Antispyware support with Enhanced Endpoint Security	Dynamically download Webroot's market-leading anti-malware software to enforce endpoint security on devices which may not be corporate-assigned computers being used for network access	Protects endpoints from infection in real-time from spyware and thereby protects corporate resources from harm during network access
SMS Auto-remediation	Automatically remediate non-compliant endpoints by updating software applications that do not comply to corporate security policies. Dynamically initiates an update of these software applications on the endpoint using the Microsoft SMS protocol.	Improves productivity of remote users who will gain immediate access to the corporate network without having to wait for periodic updates of software applications, and ensures compliance with corporate security policies.
Host Checker	Client computers can be checked both prior to and during a session to verify an acceptable security posture requiring installed/running endpoint security applications (antivirus, firewall, other). Also supports custom-built checks including verifying ports opened/closed, checking files/process and validating their authenticity with Message Digest 5 (MD5) hash checksums, verifying registry settings, machine certifications, and more.	Verifies/ensures that each endpoint device meets corporate security policy requirements before granting access, remediating devices and quarantining users when necessary.
Host Checker Application Programming Interface (API)	Created in partnership with best-of-breed endpoint security vendors. Enables enterprises to enforce an endpoint trust policy for managed PCs that have personal firewall, antivirus clients, or other installed security clients, and quarantine non-compliant endpoints.	Uses current security policies with remote users and devices; easier management.
Trusted Network Connect (TNC) support on Host Checker	Allows interoperability with diverse endpoint security solutions from antivirus to patch management to compliance management solutions.	Enables customers to leverage existing investments in endpoint security solutions from third-party vendors.
Policy-based enforcement	Allows the enterprise to establish trustworthiness of non-API-compliant hosts without writing custom API implementations or locking out external users such as customers or partners that run other security clients.	Enables access to extranet endpoint devices like PCs from partners that may run security clients different from that of the enterprise.
Hardened security appliance	Designed on a purpose-built operating system.	Not designed to run any additional services and is thus less susceptible to attacks; no back doors to exploit or hack.
Security services employ kernel-level packet filtering and safe routing	Undesirable traffic is dropped before it is processed by the TCP stack.	Ensures that unauthenticated connection attempts such as malformed packets or denial of service (DoS) attacks are filtered out.
Secure virtual workspace	A secure and separate environment for remote sessions that encrypts all data and controls I/O access (printers, drives).	Ensures that all corporate data is securely deleted from a kiosk or other unmanaged endpoint after a session.
Cache cleaner	All proxy downloads and temp files installed during the session are erased at logout.	Ensures that no potentially sensitive session data is left behind on the endpoint machine.
Data trap and cache controls	Rendering of content in non-cacheable format.	Prevents sensitive metadata like cookies, headers, and form entries from leaving the network.
Coordinated threat control	Enables SA Series and IDP Series appliances to tie the session identity of the SSL VPN with the threat detection capabilities of IDP Series, taking automatic action on users launching attacks.	Effectively identifies, stops, and remediates both network and application-level threats within remote access traffic.

Performance Scalability with the SA6500 FIPS

The SA6500 FIPS is specifically designed to accommodate large numbers of users with complex application needs, and provides application performance optimization via compression algorithms and hardware-based SSL acceleration. These features allow the appliance to process large, simultaneous transaction loads while minimizing perceptible latency to users.

Table 5: SA6500 FIPS Performance Scalability

FEATURE	FEATURE DESCRIPTION	BENEFIT
Built-in hardware-based SSL acceleration	Offloads compute-intensive encrypt/decrypt process from the CPU.	Enhanced performance.
Optional 4-port Small Form-factor Pluggable (SFP) interface card with flexibility to select SX, LX, and copper-based Gigabit Interface Connector (GBIC) interfaces	Fully redundant/meshed configuration of SSL VPN appliances with multiple load balancers.	Optimized uptime.
4-port copper 10/100/1000 interface card	Provides high-speed Gigabit Ethernet connections to internal switches.	Enables link redundancy to the LAN.
Clustering	Cluster pairs or multi-unit clusters can be deployed across the LAN or across the WAN for superlative scalability with a large number of user licenses.	Access scales as the user base grows.

High Availability

The SA4500 FIPS and SA6500 FIPS appliances include a variety of unique, first-in-industry capabilities for the availability and redundancy required for mission-critical access in demanding enterprise environments.

Table 6: SA4500 FIPS and SA6500 FIPS High Availability

FEATURE	FEATURE DESCRIPTION	BENEFIT
SA4500 FIPS		
Stateful peering	Units that are part of a cluster pair synchronize system-state, user profile-state, and session-state data among a group of appliances in the cluster.	Seamless failover with minimal user downtime and loss of productivity.
Clustering	Cluster pairs multiply aggregate throughput to handle unexpected burst traffic as well as resource intensive application use. Clusters can be deployed in either active/passive or active/active modes across the LAN or across the WAN.	Superlative scalability with a large number of user licenses that scale access as the user base grows.
SA6500 FIPS		
Dual, mirrored hot swappable Serial Advanced Technology Attachment (SATA) hard drives and dual, hot swappable fans hot swappable power supplies (second power supply optional, DC power supplies available)	Ensures continuous operation in the rare event of a failure of a component.	Optimized uptime, operational convenience, high availability.
Stateful peering	Units that are part of a cluster pair synchronize system-state, user profile-state, and session-state data among a group of appliances in the cluster.	Seamless failover with minimal user downtime and loss of productivity.
Clustering	Cluster pairs multiply aggregate throughput to handle unexpected burst traffic as well as resource-intensive application use. Clusters can be deployed in either active/passive or active/active modes across the LAN or across the WAN.	Superlative scalability with a large number of user licenses that scale access as the user base grows.

Streamlined Management and Administration

The SA4500 FIPS and SA6500 FIPS appliances include a variety of features available from a central management console at the click of a button. These benefits are extended across clustered devices, with the addition of Juniper Networks NSM Central Manager, part of the advanced feature set. NSM Central Manager is a robust product with an intuitive web-based UI designed to facilitate the task of configuring, updating, and monitoring SA Series appliances whether within a single device, local cluster, or across a global cluster deployment.

Table 7: SA4500 FIPS and SA6500 FIPS Streamlined Management and Administration

FEATURE	FEATURE DESCRIPTION	BENEFIT
Constrained delegation	When a user logs into the SA Series with a credential that cannot be proxied through to the backend server, the SA Series will retrieve a Kerberos ticket on behalf of the user from the Active Directory infrastructure. The ticket will be cached on the SA Series throughout the session. When the user accesses Kerberos-protected applications, the SA Series will use the cached Kerberos credentials to log the user into the application without prompting for a password.	Eliminates the need for companies to manage static passwords resulting in reduced administration time and costs.
Advanced SSO enhancements	SA Series will automatically authenticate remote users via Kerberos or NTLMv2 using user credentials.	Simplifies user experience by avoiding having users enter credentials multiple times to access different applications.
Juniper Networks Network and Security Manager (NSM)	Intuitive centralized user interface for configuring, updating, and monitoring SA Series appliances within a single device/cluster or across a global cluster deployment.	Enables companies to conveniently manage, configure, and maintain SA Series appliances and other Juniper devices from one central location.
Password management integration	Standards-based interface for extensive integration with password policies in directory stores (LDAP, Microsoft Active Directory, NT, and others).	Leverage existing servers to authenticate users; users can manage their passwords directly through the SA Series interface.
Web-based Single Sign-On (SSO) BASIC Auth and NTLM	Allows users to access other applications or resources that are protected by another access management system without re-entering login credentials.	Alleviates the need for end users to enter and maintain multiple sets of credentials for web-based and Microsoft applications.
Web-based SSO forms-based, header variable-based, SAML-based	Ability to pass user name, credentials, and other customer-defined attributes to the authentication forms of other products and as header variables.	Enhances user productivity and provides a customized experience.
Role-based delegation	Granular role-based delegation lessens IT bottlenecks by allowing administrators to delegate control of diverse internal and external user populations to the appropriate parties.	Associates real-time control with business, geographic, and functional needs.
Easy-to-edit role mapping and resource authorization policies	Administrators can copy and reuse existing policies.	Simplifies the process of setting up complex, multi-variable polices or administration for multiple types of groups/roles.

Lower TCO

In addition to enterprise-class security benefits, the SA4500 FIPS and SA6500 FIPS appliances have many features that enable low total cost of ownership.

Table 8: SA4500 FIPS and SA6500 FIPS Lower TCO

FEATURE	FEATURE DESCRIPTION	BENEFIT
WX Client Integration	When deployed in conjunction with the Juniper Networks WX Client, the SA Series can dynamically provision secure, accelerated remote access for employees, partners, and contractors. For more details on WX Client, please visit **www.juniper.net/application-acceleration.**	Improves end user productivity by providing LAN-like performance for accessing applications and files via Network Connect regardless of where the end user is located.
Based on industry-standard protocols and security methods	No installation or deployment of proprietary protocols is required.	Investment in the SA4500 FIPS AND SA6500 FIPS can be leveraged across many applications and resources over time.
Extensive directory integration and broad interoperability	Existing directories can be leveraged for authentication and authorization, enabling granular secure access without recreating those policies.	Existing directory investments can be leveraged with no infrastructure changes; no API's for directory integration are needed, as functionality is all native/built-in.
Integration with strong authentication and identity and access management platforms	Ability to support SecurID, Security Assertion Markup Language (SAML), and PKI/digital certificates.	Leverages existing corporate authentication methods to simplify administration.
Cross-platform support	Ability for any platform to gain access to resources such as Windows, Mac, Linux, or mobile devices.	Provides flexibility in allowing users to access corporate resources from any type of device using any type of operating system.

Table 8: SA4500 FIPS and SA6500 FIPS Lower TCO (continued)

FEATURE	FEATURE DESCRIPTION	BENEFIT
Multiple hostname support	Provides the ability to host different virtual extranet websites from a single SA4500 FIPS or SA6500 FIPS SSL VPN Appliance.	Saves the cost of incremental servers, eases management overhead, and provides a transparent user experience with differentiated entry URLs.
Customizable user Interface	Creation of completely customized sign-in pages.	Provides an individualized look for specified roles, streamlining the user experience.
Secure Meeting	Secure any time, anywhere, cost-effective online Web conferencing and remote control PC access.	Quickly schedule online meetings without any training or special deployments needed. Help desk staff or customer service reps can provide remote assistance to users by remotely controlling their PC without requiring users to install any software.
"In Case of Emergency" (ICE)	Provides licenses for a large number of additional users on an SA Series SSL VPN Appliance for a limited time when a disaster or epidemic occurs.	Enables a company to continue business operations by maintaining productivity, sustaining partnerships, and delivering continued services to customers when the unexpected happens.
Instant Virtual Systems (IVS)	Allows IT administrators to provision logically independent SSL VPN gateways within a single appliance/cluster.	Enables service providers (SPs) to offer network-based SSL VPN managed services to multiple customers from a single device or cluster, as well as enabling enterprises to completely segment SSL VPN traffic between multiple groups.

SA4500 FIPS

SA6500 FIPS

Specifications

	SA4500 FIPS	SA6500 FIPS
Upgrade Options		
Software	· Secure Meeting Upgrade Option · Instant Virtual Systems (IVS) Upgrade Option · In Case of Emergency (ICE) Upgrade Option · Additional Users Upgrade Option · Clustering Upgrade Option · Enhanced Endpoint Security Option	· Secure Meeting Upgrade Option · Instant Virtual Systems (IVS) Upgrade Option · In Case of Emergency (ICE) Upgrade Option · Additional Users Upgrade Option · Clustering Upgrade Option · Enhanced Endpoint Security Option
Hardware	None	· Field upgradeable secondary 400 W power supply · Field replaceable 80 gigabyte hot swappable hard disk · Field replaceable hot swappable fan · 4-port small form-factor pluggable (SFP) GBIC transceiver - 1000BASE-T RJ45 copper - 1000BASE-SX fiber - 1000BASE-LX fiber
Technical Specifications		
Dimensions (W x H x D)	17.26 x 1.75 x 14.5 in (43.8 x 4.4 x 36.8 cm)	17.26 x 3.5 x 17.72 in (43.8 x 8.8 x 45 cm)
Weight	15.6 lb (7.1 kg) typical (unboxed)	26.4 lb (12 kg) typical (unboxed)
Material	18 gauge (.048 in) cold-rolled steel	18 gauge (.048 in) cold-rolled steel
Fans	Three 40 mm ball bearing fans, One 40 mm ball bearing fan in power supply	Two 80 mm hot swap, One 40 mm ball bearing fan in power supply
Rack-mountable	19 inches, 1U	19 inches, 1U
Panel Display	· Power LED, HD Activity, HW Alert · FIPS Status LED · HSM Status LED	· Power LED, HD Activity, HW Alert · HD Activity and Fail LED on Drive Tray · FIPS Status LED · HSM Status LED
PS fail	No	No
HDD activity and RAID status LEDs	No	No
Ports		
Network	· Two RJ-45 Ethernet: 10/100/1000 full or half-duplex (auto-negotiation) · Fast Ethernet: IEEE 802.3u compliant · Gigabit Ethernet: IEEE 802.3z or IEEE 802.3ab compliant	· Management: One RJ-45 Ethernet – 10/100/1000 full or half-duplex (auto-negotiation) · Traffic – Four RJ-45 Ethernet – full or half-duplex (auto-negotiation); for link redundancy to internal switches – SFP module optional · Fast Ethernet: IEEE 802.3u compliant · Gigabit Ethernet: IEEE 802.3z or IEEE 802.3ab compliant
Console	One RJ-45 serial console port	One RJ-45 serial console port
Power		
AC Power Wattage	Max, 300 Watts	Max, 400 Watts
AC Power Voltage	100-240 VAC, 50-60 Hz, 2.5 A	100-240 VAC, 50-60 Hz, 2.5 A
System Battery	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell
Efficiency	80% minimum, at full load	80% minimum, at full load
Mean time between failures (MTBF)	72,000 hours	98,000 hours
Environment		
Operating temp	41° to 104° F (5° to 40° C)	41° to 104° F (5° to 40° C)
Storage temp	-40° to 158° F (-40° to 70° C)	-40° to 158° F (-40° to 70° C)
Relative humidity (operating)	8% to 90% noncondensing	8% to 90% noncondensing
Relative humidity (storage)	5% to 90% noncondensing	5% to 90% noncondensing
Altitude (operating)	10,000 ft (3,048 m) maximum	10,000 ft (3,048 m) maximum
Altitude (storage)	40,000 ft (12,192 m) maximum	40,000 ft (12,192 m) maximum

Specifications (continued)

	SA4500 FIPS	SA6500 FIPS
Certifications		
Common Criteria EAL3+ certification	Yes	Yes
Safety certifications	EN60950-1:2001+ A11, UL60950-1:2003, CAN/CSA C22.2 No. 60950-1-03, IEC 60950-1:2001	EN60950-1:2001+ A11, UL60950-1:2003, CAN/CSA C22.2 No. 60950-1-03, IEC 60950-1:2001
Emissions certifications	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A
Warranty	90 days; Can be extended with support contract	90 days; Can be extended with support contract

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster rollouts of new business models and ventures. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services/.**

Ordering Information

MODEL NUMBER	DESCRIPTION
SA4500 FIPS	
Base System	
SA4500FIPS	SA4500 FIPS Base System
User Licenses	
SA4500-ADD-50U	Add 50 simultaneous users to SA4500 FIPS
SA4500-ADD-100U	Add 100 simultaneous users to SA4500 FIPS
SA4500-ADD-250U	Add 250 simultaneous users to SA4500 FIPS
SA4500-ADD-500U	Add 500 simultaneous users to SA5000 FIPS
SA4500-ADD-1000U	Add 1,000 simultaneous users to SA4500 FIPS
Feature Licenses	
SA4500-MTG	Secure Meeting for SA4500 FIPS
SA4500-IVS	Instant Virtual System for SA4500 FIPS
SA4500-ICE	In Case of Emergency License for SA4500 FIPS
SA4500-ICE-CL	In Case of Emergency Clustering License for SA4500 FIPS
Clustering Licenses	
SA4500-CL-50U	Clustering: Allow 50 users to be shared from another SA4500 FIPS
SA4500-CL-100U	Clustering: Allow 100 users to be shared from another SA4500 FIPS
SA4500-CL-250U	Clustering: Allow 250 users to be shared from another SA4500 FIPS
SA4500-CL-500U	Clustering: Allow 500 users to be shared from another SA4500 FIPS
SA4500-CL-1000U	Clustering: Allow 1000 users to be shared from another SA4500 FIPS
Accessories	
UNIV-MR1U-RAILKIT	Rack mount kit for SA2500 or SA4500 FIPS

MODEL NUMBER	DESCRIPTION
SA6500 FIPS	
Base System	
SA6500FIPS	SA6500 FIPS Base System
User Licenses	
SA6500-ADD-100U	Add 100 simultaneous users to SA6500 FIPS
SA6500-ADD-250U	Add 250 simultaneous users to SA6500 FIPS
SA6500-ADD-500U	Add 500 simultaneous users to SA6500 FIPS
SA6500-ADD-1000U	Add 1,000 simultaneous users to SA6500 FIPS
SA6500-ADD-2500U	Add 2,500 simultaneous users to SA6500 FIPS
SA6500-ADD-5000U*	Add 5,000 simultaneous users to SA6500 FIPS
SA6500-ADD-7500U*	Add 7,500 simultaneous users to SA6500 FIPS
SA6500-ADD-10000U*	Add 10,000 simultaneous users to SA6500 FIPS
*Multiple SA6500's required	
Feature Licenses	
SA6500-MTG	Secure Application Manager and Network Connect for SA6500 FIPS
SA6500-IVS	Advanced for SA6500 FIPS
SA6500-ICE	Secure Meeting for SA6500 FIPS
SA6500-ICE-CL	In Case of Emergency clustering license for SA6500 FIPS
Clustering Licenses	
SA6500-CL-100U	Clustering: Allow 50 users to be shared from another SA6500 FIPS
SA6500-CL-250U	Clustering: Allow 100 users to be shared from another SA6500 FIPS
SA6500-CL-500U	Clustering: Allow 250 users to be shared from another SA6500 FIPS
SA6500-CL-1000U	Clustering: Allow 1000 users to be shared from another SA6500 FIPS
SA6500-CL-2500U	Clustering: Allow 2500 users to be shared from another SA6500 FIPS
SA6500-CL-5000U	Clustering: Allow 5000 users to be shared from another SA6500 FIPS
SA6500-CL-7500U	Clustering: Allow 7500 users to be shared from another SA6500 FIPS
SA6500-CL-10000U	Clustering: Allow 10000 users to be shared from another SA6500 FIPS

Ordering Information (continued)

MODEL NUMBER	DESCRIPTION
Accessories	
UNIV-PS-400W-AC	Field upgradeable secondary 400 W power supply for SA6500 FIPS
UNIV-80G-HDD	Field replaceable 80 gigabyte hard disk for SA6500 FIPS
UNIV-MR2U-FAN	Field replaceable fan for SA6500 FIPS
UNIV-MR2U-RAILKIT	Rack mount kit for SA6500 FIPS
UNIV-SFP-FSX	Mini-GBIC transceiver - fiber SX for SA6500 FIPS
UNIV-SFP-FLX	Mini-GBIC transceiver - fiber LX for SA6500 FIPS
UNIV-SFP-COP	Mini-GBIC transceiver - copper for SA6500 FIPS
SA6500-IOC	GBIC I/O card
Enhanced Endpoint Security Licenses for SA4500 FIPS and SA6500 FIPS	
ACCESS-EES-10U-1YR	Enhanced Endpoint Security subscription, 10 concurrent users, 1-year
ACCESS-EES-25U-1YR	Enhanced Endpoint Security subscription, 25 concurrent users, 1-year
ACCESS-EES-50U-1YR	Enhanced Endpoint Security subscription, 50 concurrent users, 1-year
ACCESS-EES-100U-1YR	Enhanced Endpoint Security subscription, 100 concurrent users, 1-year
ACCESS-EES-250U-1YR	Enhanced Endpoint Security subscription, 250 concurrent users, 1-year
ACCESS-EES-500U-1YR	Enhanced Endpoint Security subscription, 500 concurrent users, 1-year
ACCESS-EES-1000U-1YR	Enhanced Endpoint Security subscription, 1,000 concurrent users, 1-year
ACCESS-EES-2500U-1YR	Enhanced Endpoint Security subscription, 2,500 concurrent users, 1-year
ACCESS-EES-5000U-1YR	Enhanced Endpoint Security subscription, 5,000 concurrent users, 1-year
ACCESS-EES-7500U-1YR	Enhanced Endpoint Security subscription, 7,500 concurrent users, 1-year
ACCESS-EES-10U-2YR	Enhanced Endpoint Security subscription, 10 concurrent users, 2-year
ACCESS-EES-25U-2YR	Enhanced Endpoint Security subscription, 25 concurrent users, 2-year

MODEL NUMBER	DESCRIPTION
Enhanced Endpoint Security Licenses for SA4500 FIPS and SA6500 FIPS (coninued)	
ACCESS-EES-50U-2YR	Enhanced Endpoint Security subscription, 50 concurrent users, 2-year
ACCESS-EES-100U-2YR	Enhanced Endpoint Security subscription, 100 concurrent users, 2-year
ACCESS-EES-250U-2YR	Enhanced Endpoint Security subscription, 250 concurrent users, 2-year
ACCESS-EES-500U-2YR	Enhanced Endpoint Security subscription, 500 concurrent users, 2-year
ACCESS-EES-1000U-2YR	Enhanced Endpoint Security subscription, 1,000 concurrent users, 2-year
ACCESS-EES-2500U-2YR	Enhanced Endpoint Security subscription, 2,500 concurrent users, 2-year
ACCESS-EES-5000U-2YR	Enhanced Endpoint Security subscription, 5,000 concurrent users, 2-year
ACCESS-EES-7500U-2YR	Enhanced Endpoint Security subscription, 7,500 concurrent users, 2-year
ACCESS-EES-10U-3YR	Enhanced Endpoint Security subscription, 10 concurrent users, 3-year
ACCESS-EES-25U-3YR	Enhanced Endpoint Security subscription, 25 concurrent users, 3-year
ACCESS-EES-50U-3YR	Enhanced Endpoint Security subscription, 50 concurrent users, 3-year
ACCESS-EES-100U-3YR	Enhanced Endpoint Security subscription, 100 concurrent users, 3-year
ACCESS-EES-250U-3YR	Enhanced Endpoint Security subscription, 250 concurrent users, 3-year
ACCESS-EES-500U-3YR	Enhanced Endpoint Security subscription, 500 concurrent users, 3-year
ACCESS-EES-1000U-3YR	Enhanced Endpoint Security subscription, 1,000 concurrent users, 3-year
ACCESS-EES-2500U-3YR	Enhanced Endpoint Security subscription, 2,500 concurrent users, 3-year
ACCESS-EES-5000U-3YR	Enhanced Endpoint Security subscription, 5,000 concurrent users, 3-year
ACCESS-EES-7500U-3YR	Enhanced Endpoint Security subscription, 7,500 concurrent users, 3-year

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at **www.juniper.net**.

Notes

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

1000264-008-EN May 2010

Printed on recycled paper